UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSHUA RUPNOW, PETER SZOSTAK, and all others similarly situated, Plaintiffs, v. E*TRADE SECURITIES, LLC, Defendant.	Civil Action No. 1:19-cv-10942-VSB

~~[PROPOSED]~~ STIPULATED PROTOCOL GOVERNING DISCOVERY AND PRODUCTION OF DOCUMENTS AND ELECTRONICALLY STORED INFORMATION

The parties in the above-captioned litigation (collectively, "the Parties"), by and through their respective counsel, have jointly stipulated to the terms of this Stipulated Protocol Governing Discovery and Production of Documents and Electronically Stored Information (the "ESI Protocol"). The ESI Protocol shall apply to all discovery in this case (the "Litigation") including production of Electronically-Stored Information ("ESI") and hard-copy documents. By stipulating to this Protocol, no Party is waiving any objection that could otherwise be made in response to a discovery request.

I. SCOPE

A. Rule 34.

Federal Rule of Civil Procedure 34 permits the Parties to specify the form or forms in which ESI is to be produced. Pursuant to Rule 34, this ESI Protocol shall govern the production of hard copy documents and other physical materials ("Documents") and ESI by the Parties in the Litigation. The ESI Protocol does not alter the Parties' obligations to comply with the applicable

Federal Rules of Civil Procedure and any applicable local rules regarding the production of Documents and ESI.

B. Limitations of Protocol.

Nothing in this ESI Protocol establishes any agreement regarding the subject matter or scope of discovery in this Litigation, or the relevance, authenticity, or admissibility of any Documents or ESI. Nothing in this ESI Protocol shall be interpreted to require production of Documents or ESI protected from disclosure by the attorney-client privilege, work product doctrine, common interest privilege, or any other applicable protection or privilege. Nor shall this ESI Protocol be interpreted to require production of Documents or ESI prohibited from disclosure under any similar law, regulation, rule, or court order.

C. Non-Waiver.

The Parties do not waive any objections to the production, discoverability, or confidentiality of Documents, ESI, or any other discovery materials, including but not limited to: objections regarding the proportionality of the discovery request or the burden, overbreadth, or relevance of Documents, ESI, or any other discovery materials.

D. Variance from Protocol.

Any practice or procedure set forth herein may be varied by written agreement of the Parties.

II. DISCOVERY OF ESI

A. Responsive ESI

The Parties will take reasonable steps to produce responsive ESI stored on reasonably accessible sources. Reasonably accessible sources of ESI include, but are not limited to, computer hard drives, email accounts, and shared network drives. Notwithstanding anything to the contrary

herein, the parties have no obligation to produce the following document types are not discoverable in the Litigation except upon a showing of good cause, or unless otherwise agreed by the Parties or ordered by the Court: deleted, fragmented, residual data, or online access data such as temporary internet files, history, cache, or cookies, temporary data stored in the random access memory ("RAM") of a computer, or ESI that can only be obtained by forensic analysis of deleted or over-written data on a device.

B. Custodians and Search Terms.

The Parties will confer promptly and in good faith to seek to reach agreement regarding the identification of document and/or ESI custodians and the identification and application of search terms. The producing party will review and produce all responsive, non-privileged inclusive documents, subject to the terms of the parties' Stipulated Protective Order entered by the Court on March 24, 2022, located at Docket Entry No. 40.

C. Deduplication.

Where practicable, the Parties shall use commercially acceptable methods (e.g., MD5 or SHA-1 hash values) to identify duplicate ESI and globally de-duplicate ESI. Parties may only de-duplicate documents globally and contextually, meaning that documents are exact duplicates if a document family or stand-alone file has a matching MD5 or SHA-1 hash value as compared against the same document type (i.e., family, or stand-alone file). "Duplicate ESI" means exact duplicates based on the files' MD5 or SHA-1 Hash Value. If there is any handwriting or other alteration of a document, it shall not be considered a duplicate under this provision; the Parties will not treat a document containing handwritten notes, highlighting, or any other markings as a duplicate of a non-marked or annotated version of the same document. The Parties will not de-duplicate loose electronic documents or Hard Copy Information against email attachments. A

Party may de-duplicate ESI across its custodians or sources, but if that option is exercised, the Party shall identify each custodian who had a copy of the produced document in the ALL CUSTODIANS field and in the ALL CUSTODIAN FILE PATH field in the Metadata load file to indicate where the duplicate files were stored (folder name/structure). A Party may only de-duplicate "exact duplicate" documents and may not de-duplicate "near duplicate" documents, both of the quoted terms in this sentence being given their ordinary meaning in the e-discovery field. In order to reduce the volume of entirely duplicative content within email threads, the Producing Party may, but is not required to use email thread suppression, provided however, that an email that includes an attachment or content in the BCC or other blind copy field shall not be treated as a lesser-included version of an email that does not include the attachment or content, even if all remaining content in the email is identical.

For the avoidance of doubt, only email messages for which the parent document and all attachments are contained in the more inclusive email message will be considered less inclusive email messages that need not be produced; if the later message contains different text or content (such as, as non-exhaustive examples, where the later message adds in-line comments to the body of the earlier message, or does not include an attachment that was part of the earlier message), the earlier message must be produced.

III. FORM OF PRODUCTION

A. Hard Copy Information.

Documents will be scanned or otherwise converted into electronic form from paper documents as set forth in the following sections.

1. TIFF.

All Documents shall be scanned to single page Group 4, TIFF format, at least 300 dpi and 8 ½ x 11 inch page size (except for Documents requiring higher resolution or different page size), searchable Unicode Text Files, an Unicode delimited searchable metadata file (.dat file), and an image load file that can be loaded into commercially acceptable production software (e.g., Relativity). Each image file should have a unique file name which shall be the Bates number of the page.

2. Unitization, Organization, and other Production Specifications.

In scanning paper Documents, images of Documents will be organized according to the manner in which they were maintained in the ordinary course of business to the extent practicable, including, where available, copies of file folders, envelopes, or labels or other identifying marks on the containers in which the Documents were maintained. Distinct documents should not be merged into a single record, and single documents should not be split into multiple records. In the case of an organized compilation of separate hardcopy documents—for example, a binder containing several separate documents behind numbered tabs—the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be maintained, such as, for example, by properly coding the family fields as described in this Protocol. In addition, where a paper document has "post-it" notes or any other affixed labels, the information on the label and/or note shall be scanned and produced to the extent practicable. Document boundaries will be logically determined. The Parties will undertake reasonable efforts to, or have their vendors, unitize documents correctly, and will commit to address situations of improperly unitized documents.

B. Electronically Stored Information (ESI).

The parties will produce ESI, whenever possible, in single-page Group IV TIFF image with accompanying metadata fields, imaged at 300 dpi, with the exception of the file types identified in B.3. Each imaged version of an electronic document will be created directly from the original electronic document. Documents that contain languages other than English, in whole or in part, shall be produced in the original language(s). The document's original orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Bates numbers and redactions (to the extent they are necessary) should be burned into the image as set forth below. TIFF image files should be provided in an "Images" folder.

1. Bates Numbers & Unique IDs.

Each TIFF image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be padded to 8 digits, taking into consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, the Producing Party will so note in a cover letter or production log accompanying the production, and with the insertion of slip sheets indicating that the gap in Bates numbers and the reason(s) therefor. Page-level Bates numbers will be branded on TIFF images and additional legends applied where applicable. If documents that the Parties have agreed to produce in native format per this protocol are to be used at depositions or attached to pleadings or papers filed with the Court, the party offering the native document must identify the document as native format and provide the slip sheet provided by the producing party for each native file including Bates stamp, Protective Order designation, as appropriate, and agreed upon metadata fields for authentication purposes.

2. Parent-Child Relationships for ESI Documents.

Parent-child relationships (the association between an attachment and its parent document) must be preserved in such a way that a document or electronic file and any attachments are produced in the same production set and the relationships are identifiable. Embedded files in email messages are to be considered attachments. The Parties agree to provide beginning attachment and ending attachment fields in the database load file to capture the entire production number range for the parent/child(ren) documents. Attachments are to be produced contemporaneously and sequentially immediately after the parent document.

3. Native File Format Production.

The following file types, to the extent they are produced, shall be produced in their native file format with an accompanying placeholder image:

- Electronic spreadsheets (e.g., Excel);

- Computer aided design (CAD) files;

- Audio/video/multimedia files;

- PowerPoint (.ppt) files;

- Photos (jpg and jpeg); and

4. Structured Data.

To the extent a response to a non-objectionable discovery request requires production of discoverable electronic information contained in a database, it shall be produced in its native format unless not practicable, in which case the producing party shall notify the requesting party and the parties shall promptly meet to attempt to resolve the issue. If the producing party asserts that production of a database in native is not practicable, the producing party may advise of a preference to (1) produce existing reports or reports readily able to be generated from the database

that are reasonably responsive to the discovery requests, or (2) design queries in order to produce an extract from the database of relevant and responsive data in a reasonably usable and exportable electronic file (e.g., Excel, Access, CSV or Microsoft SQL server database format). Any production of a database not in its native format should be fully parsible. For enterprise database systems from which data will be produced, the parties will meet and confer as to the available data in the system, the data to be exported, and the format of production on a case by case basis. The producing party agrees to disclose the search parameters used to design the reports and/or queries prior to the production. Upon review of any such parameters and productions from structured databases, the requesting party may make reasonable requests for additional information to explain the database schema, fields, codes, abbreviations, and different report formats, and may object to this method of production. The processed native for all spreadsheets (i.e., MS Excel, .CSV, or similar), documents with "macros," and electronic information containing audio or visual components should be produced and linked to their corresponding documents by the metadata field "NATIVELINK." The requesting party may make reasonable requests for certain other electronic files and/or databases initially produced in their petrified (TIFF) format to be produced in their native format in the event that the petrified format is not reasonably usable. The requesting party shall identify the files or databases by their Bates numbers and the materials should be produced in their unaltered native format. To the extent that a native file must be redacted, the producing party may redact either the native file or produce TIFF images with burned in redactions in lieu of a Native File and TIFF placeholder image. XLS files requiring redactions shall be done on the native file. Native PowerPoint presentations that require redactions shall be produced as TIFF images, which shall include speaker notes and "hidden" slides as extracted by the software used to process the documents. Color PowerPoint presentations requiring redactions shall be converted to

color images (COLOR section at end of document) and black and white PowerPoint presentations requiring redactions shall be converted to black and white TIFF images, provided that proper grayscale printing is enabled to ensure that any dark colored text is not hidden by dark objects/drawings around the text. If the PowerPoint or slide program contains video or audio components, the video or audio will be produced as native files with the appropriate attachment relationships. Any document produced in native format, will also be produced according to the following specifications:

i. The original file name and file extension shall be preserved in the corresponding load file.

ii. The native format documents shall be accompanied by reference information, or metadata, that sets forth for each document, sufficient information to allow the Parties to track and authenticate the native format documents produced, including: (1) the name of the custodian from whose files the electronic file is produced; (2) an appropriately calculated "MD-5 Hash Value"; and (3) the original name of the file.

iii. A file produced in native format need not be imaged beyond the accompanying placeholder image referenced above, which shall include . a slipsheet containing the phrase "Produced In Native", a Bates stamp and Protective Order designation.

5. Request(s) for Additional Native Files.

If good cause exists to request production of certain files in native format, other than those specifically set forth above as required to be produced in native format, a requesting party may request such production and provide an explanation of the need for native file review. In the event of any such request, the parties shall meet and confer to attempt in good faith to resolve the request, and such request may not be unreasonably refused. Any native files that are produced shall be produced with a link in the Native Link field, along with extracted text and applicable metadata fields set forth in Paragraph 13. A TIFF placeholder indicating that the document was provided in

native format should accompany the database record. If a file has been redacted, TIFF images and OCR text of the redacted document will suffice in lieu of a native file and extracted text.

6. Redactions.

Documents containing redactions (*e.g.*, pursuant to attorney-client privilege) will be produced in TIFF image format, or the producing party may redact the native file. OCR reflecting redactions will be provided in text files. Each redaction shall be indicated clearly. The producing party may redact from any TIFF image, metadata field, or native file material that is protected from disclosure by an applicable privilege, protection or immunity. Documents with embedded objects that are redacted or withheld from production will be produced in TIFF image format. Document level text files will be named as the first Bates number of the respective document. Extracted text will be provided where it exists for non-redacted documents. If a party, with good cause, requests that certain individual documents be reproduced in native format, the producing party will produce the native version where available and appropriate.

If documents are produced containing redacted information, an electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration, or addition the content of such data including any metadata therein.

7. Color.

Documents containing color, where color is necessary to decipher the meaning, context, or content of the document, the Producing Party shall honor reasonable requests for either the production of the original source Document for inspection and copying or production of a color image of the Document.

8. Archive File Types.

Archive file types (e.g., .zip, .rar) shall be uncompressed for processing. Each file contained within an archive file shall be produced. If the archive file is itself an attachment, that parent/child relationship shall also be preserved.

9. Collaboration Software Programs.

To the extent production is sought of collaboration software program data, the parties will meet and confer to discuss the format of production of collaboration program data such as Microsoft TEAMS or Slack. The parties recognize that there is a wide variety of capabilities available, and it is difficult to assert a standard into a protocol without information as to each party's capabilities.

10. System Files.

Electronic file collection will be "De-NISTed", removing commercially available operating system and application files contained on the National Institute of Standards and Technology ("NIST") file list. Identification of NIST list matches will be through MD5 Hash value

11. Image Load Files and Data Load Files.

Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the Image Load file(s) in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. The total number of documents in a production should match the total number of records in the data load file.

12. Metadata Fields and Metadata File**.**

Each of the metadata and coding fields set forth below that can be extracted shall be produced for each document and electronically stored information. The Parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document or electronically stored information, with the exception of the following: BEG BATES, ENDBATES, BEGATTACH, ENDATTACH, CUSTODIAN,AND CONFIDENTIALITY. The metadata file shall be delimited according to the following characters:

(a) Delimiter=(ASCII:020);

(b) Text-Qualifier= p (ASCII:254); and

(c) New Line=® (ASCII:174).

The Parties shall provide the following metadata for all ESI produced: as set forth in the table below:

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
CUSTODIAN	The custodian of the document
ALL CUSTODIANS	All individual(s) that had electronic files that were removed due to de-duplication (De-Duped Custodian) The ALLCUSTODIANS field should be updated across the previous production as needed in the latest production, e.g., with an ALL CUSTODIAN.DAT overlay file containing BEGBATES and ALL CUSTODIANS
ALL CUSTODIANS FILE PATHS.	The directory structure of the original duplicate file(s). Any container name is included in the path for all individual(s) that had electronic files that were removed due to de-duplication (De-Duped Custodian) The ALLCUSTODIANSFILEPATH field should be updated

Field Name	Field Description
	across the previous production as needed in the latest production, e.g., with an ALL CUSTODIAN.DAT overlay file containing BEGBATES, ALL CUSTODIANS and ALL CUSTODIANS FILE PATHS
DOCTYPE	The type of document (hardcopy) or electronic file (e.g., Word, PDF, etc.) typically indicated by the file's extension
EXTENSION	Characters of the filename indicating the relevant portion used to open the file (file extension).
FULLPATH	The directory structure of the original file(s). Any container name is included in the path.
HASHVALUE	The MD5 or SHA-1 hash value
SUBJECT	Subject line of email
TITLE	Title from properties of document
DATE and TIME SENT	Date email was sent (format: MM/DD/YYYY); Time email was sent (UTC)
DATE and TIME RECIEVED	Date email was received (format: MM/DD/YYYY); Time email was received (UTC)
PARENT_DATE and TIME	The date and time of the parent email should be applied to the parent email and all of the email attachments
TO	All recipients that were included on the "To" line of the email
FROM	The name and email address of the sender of the email
CC	All recipients that were included on the "CC" line of the email
BCC	All recipients that were included on the "BCC" line of the email
AUTHOR	Any value populated in the Author field of the document properties
FILENAME	Filename of an electronic document (Edoc or attachment)
DATE and TIME LASTMOD	Date and time an electronic document was last modified (format: MM/DD/YYYY) (Edoc or attachment)
DATE and TIME CREATED	Date and time the document was created (format: MM/DD/YYYY) (Edoc or attachment)
NATIVELINK	Native File Link (Native Files only)
CONFIDENTIALITY	The document confidentiality designation if any
CONVERSATION ID	Unique ID linking documents of the same conversations.
REDACTED	Identifies if the file has been redacted.
TEXTLINK	Text File Link
TECHNICAL ISSUE	YES where slip sheet reads "Technical issue—file cannot be processed." Otherwise, blank.
FILE SIZE	Size of document in KB as a whole number.

Field Name	Field Description
PAGE COUNT	Number of pages in record.
EMAIL MESSAGE ID	Microsoft Outlook Message ID or similar value in other message systems.

With respect to the "AllCustodian" field, the parties agree to update this information and provide an overlay on a rolling basis and for each production, as described above.

13. Encrypted Data/Password Protected Files.

The Parties will make reasonable efforts to identify any potentially relevant ESI that is password protected or encrypted and undertake reasonable and proportional efforts to remove the key(s) password(s) in order for the documents to be searched and/or reviewed. In such cases the Producing Party shall produce the file unencrypted. The Parties are not required to provide information on passwords obtained or the manner with which password protected or encrypted files were made accessible. If the Producing Party cannot obtain the key or password through reasonable efforts, the Producing Party should provide the file's metadata in accordance with the terms of this Order and Section III.B in the production load file and a slip-sheet should be included in the image set, stating that the file is an exception.

14. Residual, Fragmented, Damaged, or Temporary Data.

Parties reserve the right to not produce the following ESI files provided the Party identifies the file metadata that meet any search term criteria: data stored in a computer's RAM, any data on unreadable or damaged disc sectors, readable data stored in proprietary format determined to be corrupted by the software capable of rendering the format, and data that would require forensic reconstruction.

15. Production Transfers.

Productions of ESI and Hard Copy documents shall be provided to the opposing party via secure file share/FTP. If a particular production is too large to be sent via FTP, the Producing Party will consider reasonable requests to provide individual productions to the opposing party on an encrypted CD, DVD, hard drive, or other electronic media. To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the Producing Party. In such cases, the Producing Party shall transmit the encryption key or password to the Requesting Party, under separate cover, contemporaneously with sending the encrypted media.

IV. PRODUCTION OF DISCOVERY MATERIALS CONTAINING POTENTIALLY PRIVILEGED OR PROTECTED INFORMATION

A. Protective Order.

The terms of the Stipulated Protective Order in this Litigation governing the inadvertent production of privileged information, work product, or otherwise protected documents also govern all production pursuant to this Stipulated Order. The production of documents is subject to the Parties' rights under the Stipulated Protective Order, the practices of the Court, and the rules to request the return of inadvertently produced documents.

B. Preservation of Information.

By preserving information for the purpose of this Litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege. Nothing in this Protocol shall be interpreted to require the disclosure of irrelevant information, nor shall anything in this Protocol be interpreted to require the disclosure of information protected by the attorney client privilege or any other privilege or immunity. The Parties do not waive any objections to the production, discoverability, relevance, admissibility, or confidentiality of documents and ESI except as expressly provided herein. Nothing in this Protocol should be interpreted to reduce the

burden of a Party to preserve documents, including, without limitation, consistent with obligations pursuant to Federal Rule of Civil Procedure 37(e).

C. Privilege Logs.

The Parties must provide a privilege log for any document, or portion of a document, withheld on the basis of privilege. As part of their privilege log, the Parties will provide the following information for each logged Document (to the extent applicable and to the extent the information does not disclose privileged information): date; the identities of the sender/author, recipient, CC, BCC, and anyone who had access to or custody of the document, including for all of the foregoing whether they are an attorney; subject line; filename; privilege type; description of the basis of the privilege and a summary of the document's or communication's subject matter in sufficient detail to enable an evaluation of the claim of privilege; and (if not otherwise clear) whether or not the Document includes attachments (and identification by Bates Nos of any such attachments, and, if the attachments are also asserted to be privileged, listing of the information just above for each such attachment). The Parties may redact or otherwise modify the metadata fields to avoid disclosing privileged information, so long as the redacted or modified entries are clearly identified and the information provided is sufficient to allow the other Party to assess the basis for the asserted privilege(s). If documents are produced containing redacted information, an electronic copy of the original, unredacted/unmodified data shall be securely preserved in such a manner as to preserve without modification, alteration, or addition the content of such data, and any metadata.

If the requesting party requires further information, it shall explain in writing the need for such information and identify, by Bates number or other unique identifier, each document for which it seeks this information. The producing party must within seven (7) calendar days either

(i) provide the requested information or (ii) challenge the request. If a party challenges a request for further information, the Parties shall meet and confer to try to reach a mutually agreeable solution.

D. No Waiver of Privilege (FRE 502(d)).

The production of privileged or work-product protected documents, electronically stored information ("ESI"), or any other information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this Litigation or in any other federal or state proceeding. This order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). The inadvertent production of privileged or protected documents or information shall be governed by the Protective Order entered by the Court in this litigation.

V. AMENDMENT – NO LIMITATION OF RIGHTS

No modifications or amendments to the ESI Protocol shall be made except upon the consent of the Parties or, in the event the Parties cannot reach agreement, the filing of a formal motion and a showing of good cause. Nothing herein shall limit a Party's right reasonably to seek agreement from the other Parties or a court ruling to modify previously agreed- upon search terms or procedures for advanced search and retrieval technologies.

VI. THIRD PARTIES

A Party that issues a subpoena upon any third-party ("Issuing Party") shall include a copy of this Protocol and the Protective Order with the subpoena. The Issuing Party shall produce a copy to all other Parties of any ESI (including any metadata) obtained under subpoena to a third party. If a third-party production is not Bates-stamped, the Issuing Party will endorse the non-Party production with unique Bates prefixes and numbering scheme prior to reproducing them to all other Parties.

SO STIPULATED AND AGREED:

By: /s/ Kent A. Bronson

Dated: May 11, 2022

MILBERG PHILLIPS GROSSMAN LLP
Andrei V. Rado
arado@milberg.com
Kent A. Bronson
kbronson@milberg.com
One Pennsylvania Plaza, Suite 1920
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

SILVER LAW GROUP
Scott Silver
ssilver@silverlaw.com
11780 West Sample Road
Coral Springs, Florida 33065
Telephone: (954) 755-4799
Facsimile: (954) 755-4684

Attorneys for Plaintiffs

By: /s/ Marc L. Greenwald

Dated: May 11, 2022

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Marc L. Greenwald
Corey Worcester
Renita Sharma
Leigha Empson
51 Madison Avenue, 22nd Floor
New York, NY 10010
Tel: (212) 849-7000
Fax: (212) 849-7100
marcgreenwald@quinnemanuel.com
coreyworcester@quinnemanuel.com
renitasharma@quinnemanuel.com
leighaempson@quinnemanuel.com

Attorneys for Defendant

SO ORDERED: Dated: May 13, 2022
New York, New York

Hon. Vernon S. Broderick
United States District Judge